



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,255	08/26/2003	Gerard Vergnaud	Q76973	3044

23373 7590 02/06/2008
SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER

KEEFER, MICHAEL E

ART UNIT	PAPER NUMBER
----------	--------------

2154

MAIL DATE	DELIVERY MODE
-----------	---------------

02/06/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

MAILED

FEB 05 2008

Technology Center 2100

Application Number: 10/647,255
Filing Date: August 26, 2003
Appellant(s): VERGNAUD ET AL.

Kelly G. Hyndman 39,234
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/28/2007 appealing from the Office action mailed 6/21/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0075844	Hagen	6-2002
--------------	-------	--------

6408336	Schneider et al.	6-2002
---------	------------------	--------

Comer, Douglas. "Internetworking with TCP/IP Vol. 1" Prentice Hall. 2000.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-16, 21-23, 25, and 27-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hagen (US 2002/0075844 A1) and Schneider et al. (US 6408336 B1) hereafter Schneider.

Regarding **claims 1 and 28** Hagen discloses:

A processing server (Network Access Server 7, Fig. 1) for allocating user terminals (user terminal 1, Fig. 1) resources of a local area network (LAN 10, Fig. 1), which server is adapted to be connected to at least one local area network access point (connection 8, WAPs 3,4, Fig. 1) and is characterized in that it includes control means adapted:

i) (Hagen groups terminals into at least two groups, one set of groupings being those MAC addresses who are located in the database, and those MAC addresses who are not located in the database. See [0052])

ii) to allocate resources of said local area network to terminals attempting to establish communication therewith as a function of whether they are classified in said first group or said second group. ([0051], lines 1-3)

Regarding **claims 2-3 and 29 as applied to claims 1 and 28** Hagen discloses:

said control means are adapted to: determine the MAC address of each terminal attempting to establish communication with said local area network (Page 4, Col. 1, lines 7-9 disclose that the NAS retrieves the MAC address from the client from a packet.)

and in that it includes means for allocating an IP address to the terminal having the MAC address determined in this way. ([0066] "The NAS router-related services preferably include ... DHCP/DHCP Relay services")

Regarding **claims 4 and 30 as applied to claims 1-2 and 28-29**, Hagen discloses:

a memory for storing a table containing primary MAC addresses associated with first terminals adapted to exchange data frames encrypted in accordance with said format. (Page 4, Col. 1, Lines 9-12, the NAS inherently has memory for storing the database)

Regarding **claims 5 and 31 and as applied to claims 1-2, 4 and 28-30**, Hagen discloses:

said table contains secondary MAC addresses associated with second terminals (8b) adapted to exchange unencrypted data frames. ([0050] describes how the MAC address is used to look up all of the permissions a terminal is allowed.)

Regarding **claims 6 and 32 and as applied to claims 1-2, 4-5 and 28-30**, Hagen discloses:

said control means (11) are adapted to determine if a MAC address extracted from a received frame is a primary or secondary MAC address and, if so, to send the allocation means (12) a request to allocate the terminal (8b) corresponding to said primary or secondary MAC address a primary IP address so that it can set up a link with at least one first remote network and one second remote network ([0158] If the mobile terminal's MAC address is found in the database, it obtains an IP address assignment for the mobile terminal, and can communicate on the private LAN or on the Internet)

and, if not, to send the allocation means (12) a request to allocate the terminal (8c) corresponding to said MAC address, referred to as a third terminal, a secondary IP address so that it can set up a connection with at least one second remote terminal. ([0052] if the MAC address is not located in any database, it is assigned a temporary IP address; [0158] If the mobile terminal's MAC address is found in the database, it obtains an IP address assignment for the mobile terminal. [0107] lines 27-28 state that unregistered users may be given some kind of network access, i.e. being allowed to connect to a second remote terminal)

Regarding **claims 7 and 33 as applied to claims 1-2, 4 and 28-30**, Hagen discloses:

said first terminals are associated with said first remote network. (Note Fig. 13, where first terminals are private users 23)

Art Unit: 2154

Regarding **claim 8 and 34 as applied to claims 1-2, 4, 7, 28-30 and 33** Hagen discloses:

said terminals (8b) belong to known users of said first remote network. ([0107] states that one of the user terminal groupings is that of “home or local users” who are clients of the service providers private network, thus, the terminal belongs to a user of the first remote network.)

Regarding **claims 9 and 35 as applied to claims 1-2, 4, 6, 28-30, and 32** Hagen discloses:

each first remote network is selected from the group comprising private networks, IP data networks, and public switched telephone networks (PSTN), and in that each second remote network is selected from the group comprising IP data networks and public switched telephone networks (PSTN). (Fig. 13, Note the private LAN, the PSTN and the internet, an IP network)

Regarding **claims 10 and 36 as applied to claims 1 and 28**, Hagen discloses:

said control means (ii) are adapted to allocate at least two priority levels for allocation of resources of the local area network (WLAN) according to whether communications are encrypted in accordance with said chosen format or not. ([0097] BAM handles queuing between public access subscribers and private network clients, and also the allocation and throttling of bandwidth for public access subscribers and private network clients.)

Regarding **claims 11 and 37 as applied to claims 1, 10, 28, and 36**, Hagen discloses:

the MAC addresses in said table are stored in corresponding relationship to at least one priority level. (Fig. 2 shows the contents of the table, which can be different for each MAC address, included wherein is policy table 3500, which provides for items like Bandwidth Policy.)

Regarding claims 12 and 38 and as applied to claims 1, 10-11, 28, and 36-37,

Hagen discloses:

said priority levels comprise at least one first priority level allocated to first terminals (8a) associated with primary MAC addresses and one second priority level allocated to second terminals (8b) associated with secondary MAC addresses. (it is disclosed that specifically public access subscribers and private network clients could have two separate levels of priority in [0097].)

Regarding claims 13 and 39 as applied to claims 1, 10-12, 28, and 36-38

Hagen discloses:

said control means (ii) are adapted to allocate a third priority level for allocation of resources of the local area network to said third terminals (8c) setting up communications not encrypted in accordance with said chosen format and whose MAC address is not in said table. (Third terminals whose address are not in the table are allocated a priority, as shown in lines 5-8 as "unregistered users".)

Regarding claims 14 and 40 as applied to claims 1, 10-11, 28, and 36, Hagen discloses:

Art Unit: 2154

said priority levels apply at least to a bandwidth and said bandwidth decreases from the first level to the third level. ([0107] gives a greatest to least list of bandwidth allocation classes in lines 5-8.)

Regarding **claims 15 and 41 as applied to claims 1, 10-11, 14, 28, 36, and 40**,
Hagen discloses:

said control means (ii) send said access point (I) data representative of said bandwidth assigned to a designated terminal (8) and said access point allocates the corresponding resources to said designated terminal. (In [0185], it is disclosed in lines 11-14 that if the NAS is not the router, the NAS must update the QoS parameters on the router.)

Regarding **claims 16 and 42 as applied to claims 1, 10, 28, 36, and 40-41**,
Hagen discloses:

said control means (li) are adapted to modify an allocated priority level as a function of the available resources of said local area network (WLAN). (Page 12 Col 2, lines 15-20)

Regarding **claim 21 and as applied to claim 1**, Hagen discloses:

A router, characterized in that it includes a processing server according to claim 1. (In [0185] lines 11-12, states "If the NAS is not the router...", which implies that the NAS can be a router.)

Regarding **claim 22 and as applied to claim 1**, Hagen discloses:

A local area network access point, characterized in that it includes a processing server according to claim 1. ([0054] discloses that the NAS may be implemented as a stand-alone device or as part of a WAP)

Regarding **claim 23 and as applied to claim 1**, Hagen discloses:

A communication installation including at least one local area network accessible via at least one access point, at least one first remote network, and at least one second remote network, which installation is characterized in that it includes a processing server according to claim 1 connected to said access point and to said first and second remote networks. (See Fig. 1, Note that LAN 10 is accessible via the NAS from the access point; note that the NAS is connected to the access point and the Internet and the Telephone ISDN/PSTN).

Regarding **claim 25 and as applied to claim 23**, Hagen discloses:

said processing server is connected to said first remote network via a virtual private network. (In [0217] and [0218] Hagen discloses that the connection to other networks may be encrypted using IPsec, or IPsec tunnels (i.e. VPN).)

Regarding **claim 26 and as applied to claim 23**, Hagen discloses:

said processing server is connected to said first remote network via a remote access server. (In [0217] and [0218] Hagen discloses that the connection to other networks may be enabled by RADIUS or DIAMETER (i.e. remote access services, which would need a remote access server to connect to).)

Regarding **claim 27 and as applied to claim 23**, Hagen discloses:

each first remote network is chosen from the group comprising private networks, IP data networks, and public switched telephone networks (PSTN) and in that each second remote network is selected from the group comprising IP data networks and public switched telephone networks (PSTN). (See Fig. 1, the internet is an IP network, and the PSTN is a PSTN network.)

Regarding **claim 43 as applied to claim 28**, Hagen discloses:

Use of a method according to claim 28 in communication networks selected from the group comprising PSTN, PLMN and Internet (IP) public networks and PABX private networks and private communication gateways.

Regarding **claim 44 as applied to claims 28 and 43**, Hagen discloses:

Use according to claim 43, characterized in that the PLMN public networks are mobile networks selected from the group comprising GSM, GPRS and UMTS networks.

Therefore, Hagen discloses all the limitations of claims 1-16, 21-23, and 27-42 except for the terminals being classified according to their ability to use encryption.

The general concept of classifying network clients according to their security traits is well known in the art as taught by Schneider (which teaches in Col 10 lines 6-34 that in order for a client to be able to access a network resource it must meet or exceed the trust (or encryption) level of that resource).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hagen with the teaching of terminals being classified according to their security traits as taught by Schneider in order to make the system more scalable (Schneider, Col. 5 line 66).

3. Claims 17-20 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hagen and Schneider as applied to claims 1 and 23 above, and further in view of Comer, "Internetworking with TCP/IP Vol. 1".

Regarding **claims 17-18**,

Hagen discloses that The NAS includes components necessary to connect to the network, including a third conventional network interface provided for connecting to the private network (LAN) 10. ([0062] lines 7-16)

Hagen and Schneider disclose all of the limitations of claims 17-18 except that a cabled interface is used as the third conventional network interface, and in specific, Ethernet.

The general concept of using a cabled Ethernet network interface to a LAN is well known in the art as taught by Comer. (see page 20, under heading 2.4, "Ethernet has become the most popular LAN technology", also note Fig. 2.1 which shows a cable that can be used to implement Ethernet).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the network access control system of Hagen and Schneider to include the general concept of using a cabled Ethernet network interface as taught by Comer in order to be compatible with most private networks.

Regarding claims 19-20,

Hagen discloses that radio link technology used in the system disclosed is based upon IEEE 802.11b. ([0039] lines 1-2)

Hagen and Schneider disclose all the limitations of claims 19 and 20 except that a radio link is used to interface with the LAN.

The general concept of wirelessly accessing a LAN is well known in the art as taught by Comer. (Section 2.11.5 teaches that a wide variety of radio link equipment is available to create wireless LANs.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the network access control system of Hagen and Schneider to include the general concept of using a radio link network interface as taught by Comer in order to be compatible with more private networks.

Regarding **claim 24**,

Hagen and Schneider disclose all the limitations of claim 24 except that said local area network is a wireless local area network.

The general concept of a LAN being wireless is well-known in the art as taught by Comer (Section 2.11.5 teaches the possibility of creating a wireless LAN).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the network access control system of Hagen and Schneider to include the general concept of a LAN being wireless as taught by Comer in order to service a more diverse set of private LANs.

4. Claims 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hagen and Schneider.

Regarding **claims 43-44**,

Hagen and Schneider discloses all the limitations of claims 43-44 as cited above except for specific use of the method in PSTN, PLMN, IP, and PABX private networks and private communication gateways.

The general concept of limiting access to networks is well-known in the art, and PSTN, PLMN, IP, and PABX private networks and private communication gateways are well-known networks in the art, and that GSM, GPRS, and UMTS are well-known types of PLMN networks and official notice is taken as such.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the network access limiting method of Hagen and Schneider with the fact that PSTN, PLMN, IP, and PABX private networks and private communication gateways are networks that may need to have access limited in order to secure a more diverse group of networks.

(10) Response to Argument

Applicant argues that Schneider does not teach that exclusively by encryption will access be granted to resources. Claim 1 requires that terminals are classified based off of whether they use encryption. Schneider clearly uses encryption as a standard for determining access to resources. "if the access request is encrypted, the trust level of the encryption technique used, the stronger the encryption technique the higher the trust level". (see Schnieder Column 10, lines 20-23, where encryption is listed as one of many possible factors for determining a "trust level" of a device (i.e. should it be allowed to access network resources)). The fact that a "high trust level" maybe be used in

conjunction with other criteria than encryption is not relevant to the combination of Schneider and Hagen presented by the Examiner.

Applicant argues that the trust level taught by Schneider is different than what has been claimed by Applicant. However, the Examiner is citing the concept taught by Schnieder that encryption can be used to classify terminals in order to determine whether they should be allowed to access resources (as cited above in the rejections of record, as well as the argument above.)

The Examiner's statement relies on the fact that Schneider teaches the use of encryption as a way to classify terminals for access to network resources. The fact that Schneider teaches using a combination of various other attributes of a user in addition to encryption is irrelevant to the rejection at hand, especially given the use of the transition word "comprising" in the claims.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted, **NATHAN FLYNN**
SUPERVISORY PATENT EXAMINER

MEK 1/30/2008

Conferees:

~~NATHAN FLYNN~~
~~SUPERVISORY PATENT EXAMINER~~

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100